IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Board of Patent Appeals and Interferences

Appellants:	Junbiao Zhang
Serial No.:	10/566,393
Filed:	27 January 2006
For:	Controlling Access to a Network Using Redirection
Examiner:	Jing F. Sims
Art Unit:	2437
Conf. No.:	3745

Mail Stop APPEAL BRIEF
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia, 22313-1450

APPEAL BRIEF

May it please the Honorable Board:

This is Appellant's Brief on Appeal from the rejection of Claims 1, 2, 6, 10, 25, 26, and 42-57. The Appellant waives an Oral Hearing for this appeal. Enclosed is a single copy of this Brief. The fee for this Brief has been previously paid.

Table of Contents

I. REAL PARTY IN INTERST

The real party in interest of Application Serial No.10/566,393 is the Assignee of record:

Thomson Licensing

46, Quai A. Le Gallo

F-92100 Boulogne-Billancourt

FRANCE,

as evidenced by an assignment recorded at Reel/Frame 017538/0041.

II. RELATED APPEALS AND INTERFERENCES

On 24 June 2009, the Appellant filed an appeal from a final rejection dated 11 March 2009. In response to the Appellant's Appeal Brief filed on 3 August 2009, the Examiner reopened prosecution with a rejection dated 24 November 2009, thus effectively terminating the open Appeal. This Appeal is from the Examiner's rejection of 24 November 2009. Otherwise, there are currently, and have been, no related appeals and interferences regarding Application Serial No. 10/566,393, known to the undersigned attorney.

III. STATUS OF THE CLAIMS

Claims 1, 2, 6, 10, 25, 26, and 42-57 have been rejected. Claims 3-5, 7-9, 11-13, 27-34, 36 and 41 have been allowed. Claims 14-24, 35 and 27-40 have been cancelled.

The rejection of Claims 1, 2, 6, 10, 25, 26, and 42-57 is appealed.

III. STATUS OF AMENDMENTS

All amendments have been entered and are reflected in the Claims listed in Appendix I.

IV. SUMMARY OF CLAIMED SUBJECT MATTER

Independent Claim 1 claims a method for controlling access to a network, said method comprising:

receiving, by an access point (AP) of said network, a request to access said network, said request transmitted by a client (page 6, line 30, to page 7, line 1);

re-directing, by said AP, said access request to a local server (at page 6, lines 25- 26);

associating unique data with an identifier of said client and storing a mapping of said association in said AP (page 6, line 30 to page 7, line 3);

generating a Web page by said local server requesting that said client select an authentication server (AS) and including said unique data and forwarding said generated Web page to said client (page 7, lines 4-6);

transmitting an authentication request to said selected authentication server (page 7, lines 7 to 8); and

receiving a response to said authentication request from said selected authentication server (page 7, lines 8-9).

Independent claim 25 claims a system for controlling access to a network comprising:

a client (page 6, line 30);

an access point (AP) coupled to a local server (LS) for relaying network communications to and from the client (page 4, lines 4 and 18); and

an authentication server for performing an authentication process in response to a request from the client (page 3, lines 28-29); wherein

the AP, in response to a re-directed request to access the network from the client, associates unique data with an identifier of the client and stores a mapping of the association (page 6, line 30 to page 7, line 3);

the LS transmits the unique data to the client (page 7, lines 4-6);

the authentication server, upon authenticating the client using the unique data, is operative to provide a re-direct header for access to the client including a digitally signed authentication message and authentication parameters corresponding to the unique data, the AP receiving the digitally signed retrieved re-directed URL and authentication parameters from the client and the AP further correlating the authentication parameters with the mapped association data for determining access to the network based on the results of the correlation (page 7, lines 11 to 14).

Independent Claim 42 claims a method for controlling network access, said method comprising:

receiving a request for network access (page 6, lines 25 and 26);

redirecting said request via a message (page 6, line 17);

receiving a client identifier and unique data (page 6, lines 25 to 31);

associating said unique data and said client identifier (page 6, line 30 to page 7, line 1);

receiving a re-directed universal resource locator included embedded information (page 7, lines 10-14);

generating a local digital signature using said embedded information and said association between said unique data and said client identifier (page 7, lines 12-14);

comparing said local digital signature with a digital signature received in said embedded information (page 7, lines 17-20);

granting network access if said local digital signature matches said digital signature received in said embedded in information (page 7, lines 20-21); and

deny network access if said local digital signature does not match said digital signature received in said embedded information (page 7, lines 21-22).

Independent Claim 45 claims a system for controlling network access, comprising:

means (130) for receiving a request for network access (page 6, lines 25-26);

means for redirecting (210) said request (205) via a message (220, page 6, lines 15-17);

means for receiving a client identifier and unique data (page 6, lines 30-31);

means for associating said unique data and said client identifier (page 6 line 30 to page 7, line 1);

means for receiving a redirected universal resource locator included embedded information (page 7, lines 15-17);

means for generating a local digital signature using said embedded information and said association between said unique data and said client identifier (page 7, lines 17-20);

means for comparing said local digital signature with a digital signature received in said embedded information (page 7, lines 18-20);

me for granting network access if said local digital signature matches said digital signature received in said embedded information (25, page 7, lines 20-21); and

means for deny network access if said local digital signature does not match said digital signature received in said embedded information (page 7, lines 21-22).

Independent Claim 48 claims a method for controlling network access, said method comprising:

receiving a re-directed request for network access via a message (page 6, line 17);

transmitting a client identifier and unique data (page 6, lines 30-31); and

generating a web page including embedded data (page 7, lines 4-5).

Independent Claim 51 claims a system for controlling network access, comprising:

means for receiving a redirected request for network access via a message (page 6, line 17);

means for transmitting a client identifier and unique data (page 6, line 32); and

means for generating a web page including embedded data (page 7, lines 4-5).

Independent Claim 54 claims a method for controlling network access, said method comprising:

receiving an authentication user input message (page 7, lines 7-8);

transmitting authentication input page requesting authentication information (page 7, lines 8-9);

receiving authentication credentials (page 7, lines 10-11); and

transmitting an authentication message indicating one of success and failure of an authentication process (page 7, lines 11-12).

Independent Claim 56 claims a system for controlling network access, comprising:

means for receiving an authentication user input message (page 7, lines 7-8);

means for transmitting authentication input page requesting authentication information (page 7, lines 8-9);

means for receiving authentication credentials (page 7, lines 10-11); and

means for transmitting an authentication message indicating one of success and failure of an authentication process (page 7, lines 11-12).

V. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

a) Whether Claims 48-57 are properly rejectable under 35 USC 102(b) as anticipated by US 5,708,780 to Levergood et al.

b) Whether Claims 1, 2, 6, and 10 are properly rejectable under 35 USC 103(a) as unpatentable over US 2004/0047348 to O'Neill in view of US 2003/0212800 to Jones et al.

c) Whether Claims 25 and 26 are properly rejectable under 35 USC 103(a) as unpatentable over O'Neill in view of US 6,856,800 to Henry et al.

d) Whether Claim 42 is properly rejectable under 35 USC 103(a) as unpatentable over Jones et al in view of US 7,177,839 to Claxton et al.

e) Whether Claims 43-47 are properly rejectable under 35 USC 103(a) over Jones et al in view of Claxton et al and US 2005/0114680 to Chinnaswamy et al.

VI. ARGUMENT

a) Whether Claims 48-57 are properly rejectable under 35 USC 102(b) as anticipated by US 5,708,780 to Levergood et al

Independent Claim 48 claims a method for controlling network access which includes transmitting a client identifier and unique data and generating a webpage including embedded data. Nowhere does Levergood et al show or suggest this method. Levergood et al transmits a service request from a client to a server through a network such as the Internet. Nowhere does Levergood et al show or suggest:

"generating a web page including embedded data",

as specifically recited in Claim 48. Rather, Levergood et al gives access to a web page, which webpage does not include embedded data. Levergood et al merely changes the URL of an existing page to a new page name. See column 3, lines 62-65. It is therefore clear that Levergood et al does not generate a webpage, and therefore does not affect the patentability of Claim 48.

Claims 49 and 50 are dependent from claim 48 and add further advantageous features. The Appellant submits that these subclaims are patentable as their parent Claim 48.

Similarly, nowhere does Levergood et al show or suggest:

"means for generating a webpage including embedded data",

as specifically recited in Claim 51, as explained above. It is therefore clear that the patentability of Claim 51 is not affected by Levergood et al.

Claims 52 and 53 are dependent from Claim 51 and add further advantageous features. The Appellant submits that these subclaims are patentable as their parent Claim 51.

Similarly, nowhere does Levergood et al show or suggest:

"transmitting authentication input page requesting authentication information",

as specifically set forth in Claim 54. Rather, as explained above, Levergood et al does not generate a web page requesting authentication information, but rather gives access to a web page. It is therefore clear that the patentability of claim 54 is not affected by Levergood et al.

Claim 55 is dependent from Claim 54 and adds further advantageous features. The Appelant submits that Claim 55 is patentable as its parent Claim 54.

Similarly, nowhere does Levergood et al show or suggest:

"means for transmitting authentication input page requesting authentication information",

as specifically recited in Claim 56. As explained above, Levergood et al does not generate a web page, but rather gives access to a web page. It is therefore clear that the patentability of Claim 56 is not affected by Levergood et al.

Claim 57 is dependent from Claim 56 and adds further advantageous features. The Appellant submits that Claim 57 is patentable as its parent Claim 56.

b) Whether Claims 1, 2, 6, and 10 are properly rejectable under 35 USC 103(a) as unpatentable over US 2004/0047348 to O'Neill in view of US 2003/0212800 to Jones et al.

The Examiner admits that O'Neill does not disclose generating a web page by said local server for requesting that said client select an authentication server and including said unique data and forwarding said generated web page to said client. The Examiner looks to Jones et al for such a disclosure. However, nowhere does Jones et al show or suggest:

"generating a web page by said local server requesting that said client select an authentication server",

as specifically set forth in Claim 1. Rather, Jones et al provides a gateway 112 which redirects a browser to an authentication-invite web page on which the browser submits an authentication request. Nowhere does Jones et al generate a web page by a local server. Rather, Jones et al directs a browser to an *existing* web page. It is therefore clear that even if the disclosure of O'Neill were to be combined with the disclosure of Jones et al, the patentability of Claim 1 would not be affected.

Claims 2, 6 and 10 are dependent from Claim 1 and adds further advantageous features. The Appellant submits that these subclaims are patentable as their parent Claim 1.

c) Whether Claims 25 and 26 are properly rejectable under 35 USC 103(a) as unpatentable over O'Neill in view of US 6,856,800 to Henry et al.

The Examiner admits that O'Neill does not disclose an authentication server which provides a redirect header including a digitally signed authentication, and AP (access point) receiving the digitally signed retrieved redirected URL (uniform resource locator). The Examiner looks to Figure 3 and the Abstract of Henry et al for such a disclosure.

Henry et al discloses that when a user (mobile host) enters a new network (WLAN), the user must be authenticated with its home network, which can be time consuming. Henry et al offloads a portion of the authentication process to an access point of the WLAN. Neither Figure 3 nor the Abstract of Henry et al show or suggest:

" a redirect header for access to the client including a digitally signed authentication message and authentication parameters corresponding to the

unique data, the AP receiving the digitally signed retrieved redirected URL and authentication parameters from the client and AP",

as recited in Claim 25. It is therefore clear that even if the disclosures of O'Neill and Henry et al were to be combined, the patentability of Claim 25 would not be affected.

Claim 26 is dependent from Claim 25, and adds further advantageous features. The Appellant submits that this subclaim is patentable as its parent Claim 25.

d) Whether Claim 42 is properly rejectable under 35 USC 103(a) as unpatentable over Jones et al in view of US 7,177,839 to Claxton et al.

The Examiner has noted that Jones et al does not disclose:

generating a local digital signature using said embedded information and said association between said unique data and said client identifier;

comparing said local digital signature with a digital signature received in said embedded information;

granting network access if said local digital signature matches said digital signature received in said embedded information; and

deny network access if said local digital signature does not match said digital signature received in said embedded information.

The Examiner looks to Claxton et al for this disclosure.

Claxton et al. relates to a system for accomplishing business transactions where a subscriber employees a certifying authority (issuing bank) who certifies a signing party to a relying party's bank for the relying party. Claxton et al does not generate a local digital signature. Rather, Claxton et al regenerates signatures, as explained in column 51, lines 28-30. It is therefore clear that Jones et al and Claxton et al, taken either separately or together, do not affect the patentability of Claim 42.

e) Whether Claims 43-47 are properly rejectable under 35 USC 103(a) over Jones et al in view of Claxton et al and US 2005/0114680 to Chinnaswamy et al.

Chinnaswamy et al relates to WLAN security. When a client device connects to a WLAN, the WLAN responds with a logon page which permits a customer to enter logon data. Such data is forwarded to a AAA server, which accepts or rejects the client device. Nowhere does Chinnaswamy et al generate a local digital signature, as set forth in Claim 42. It is therefore clear that Jones et al, Claxton et al and Chinnaswamy et al, taken either singly or in combination, do not affect the patentability of Claim 42. Claims 43 and 44 are dependent from Claim 42 and add further advantageous features. The Appellant therefore submits that Claims 43 and 44 are patentable as their parent Claim 42.

The Examiner has noted that Claims 45 to 47 are system claims corresponding to the method set forth in Claims 42 to 44. The Appellant therefore submits that Claims 45 to 47 are patentable as Claims 42 to 44.

The Appellant submits that all of the rejected Claims are allowable, and that the Rejection should be reversed.

Respectfully submitted,
JUNBIAO ZHANG

by: _/Daniel E. Sragow/_____
Daniel E. Sragow, Attorney
Reg. No. 22,856
(609) 734-6832

Patent Operations
Thomson Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312

APPENDIX I. APPEALED CLAIMS

1. A method for controlling access to a network, said method comprising:

receiving, by an access point (AP) of said network, a request to access said network, said request transmitted by a client;

re-directing, by said AP, said access request to a local server;

associating unique data with an identifier of said client and storing a mapping of said association in said AP;

generating a Web page by said local server requesting that said client select an authentication server (AS) and including said unique data and forwarding said generated Web page to said client;

transmitting an authentication request to said selected authentication server; and

receiving a response to said authentication request from said selected authentication server.

2. The method according to claim 1, wherein said network is a wireless Local Area network (WLAN).

3. (allowed).

4. (allowed)

5. (allowed)

6. The method according to claim 1, wherein said identifier is an address of said client.

7. (allowed)

8. (allowed)

9. (allowed)

10. The method according to claim 1, wherein said identifier is one of a physical (PHY) address of said client, a MAC address of said client and an IP address of said client.

11. (allowed)

12. (allowed)

13. (allowed).

14-24 (cancelled)

25. A system for controlling access to a network comprising:

a client;

an access point (AP) coupled to a local server (LS) for relaying network communications to and from the client; and

an authentication server for performing an authentication process in response to a request from the client; wherein

the AP, in response to a re-directed request to access the network from the client, associates unique data with an identifier of the client and stores a mapping of the association;

the LS transmits the unique data to the client;

the authentication server, upon authenticating the client using the unique data, is operative to provide a re-direct header for access to the client including a digitally signed authentication message and authentication parameters corresponding to the unique data, the AP receiving the digitally signed retrieved re-directed URL and authentication parameters from the client and the AP further correlating the authentication parameters with the mapped association data for determining access to the network based on the results of the correlation.

26. The system of claim 25, wherein the network is a wireless local area network (WLAN) comprising the access point and local server.

27. (allowed)

28. (allowed)

29. (allowed)

30. (allowed)

31. (allowed)

32. (allowed)

33. (allowed)

34. (allowed)

Claim 35. (CANCELLED)

36. (allowed)

Claims 37-40 (CANCELLED)

41. (allowed)

42. A method for controlling network access, said method comprising:

receiving a request for network access;

re-directing said request via a message;

receiving a client identifier and unique data;

associating said unique data and said client identifier;

receiving a re-directed universal resource locator included embedded information;

generating a local digital signature using said embedded information and said association between said unique data and said client identifier;

comparing said local digital signature with a digital signature received in said embedded information;

granting network access if said local digital signature matches said digital signature received in said embedded information; and

deny network access if said local digital signature does not match said digital signature received in said embedded information.

43. The method according to claim 42, wherein said unique data comprises a session identifier and a random number.

44. The method according to claim 42, wherein said embedded information further comprises a session identifier and authentication parameters.

45. A system for controlling network access, comprising:

means for receiving a request for network access;

means for re-directing said request via a message;

means for receiving a client identifier and unique data;

means for associating said unique data and said client identifier;

means for receiving a re-directed universal resource locator included embedded information;

means for generating a local digital signature using said embedded information and said association between said unique data and said client identifier;

means for comparing said local digital signature with a digital signature received in said embedded information;

means for granting network access if said local digital signature matches said digital signature received in said embedded information; and

means for deny network access if said local digital signature does not match said digital signature received in said embedded information.

46. The system according to claim 45, wherein said unique data comprises a session identifier and a random number.

47. The system according to claim 45, wherein said embedded information further comprises a session identifier and authentication parameters.

48. A method for controlling network access, said method comprising:

receiving a re-directed request for network access via a message;

transmitting a client identifier and unique data; and

generating a web page including embedded data.

49. The method according to claim 48, wherein said unique data comprises a session identifier and a random number.

50. The method according to claim 48, wherein said embedded data comprises a session identifier, a random number and authentication server selection information.

51. A system for controlling network access, comprising:

means for receiving a re-directed request for network access via a message;

means for transmitting a client identifier and unique data; and

means for generating a web page including embedded data.

52. The system according to claim 51, wherein said unique data comprises a session identifier and a random number.

53. The system according to claim 51, wherein said embedded data comprises a session identifier, a random number and authentication server selection information.

54. A method for controlling network access, said method comprising:

receiving an authentication user input message;

transmitting authentication input page requesting authentication information;

receiving authentication credentials; and

transmitting an authentication message indicating one of success and failure of an authentication process.

55. The method according to claim 54, wherein said authentication message comprises a digital signature, a session identifier, authentication parameters and a random number.

56. A system for controlling network access, comprising:

means for receiving an authentication user input message;

means for transmitting authentication input page requesting authentication information;

means for receiving authentication credentials; and

means for transmitting an authentication message indicating one of success and failure of an authentication process.

57. The system according to claim 56, wherein said authentication message comprises a digital signature, a session identifier, authentication parameters and a random number.

APPENDIX II. EVIDENCE

None

APPENDIX III. RELATED PROCEEDINGS

The Appellant asserts that there are presently no proceedings related to or affecting the instant Appeal.